

REMARKS

In the Final Office Action, the Examiner rejected claims 42-82 under 35 U.S.C. § 112, ¶ 1, for failing to comply with the written description requirement.¹ In addition, the Examiner rejected each of the claims 42-82 under 35 U.S.C. § 103(a) as being unpatentable over Viktor Fischer et al., *Two Methods of Rijndael Implementation in Reconfigurable Hardware*, 2162 Lecture Notes in Computer Science, Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems 77 (May 14-16 2001) ("Viktor") in view of U.S. Patent No. 5,261,003 ("Matsui"), and further in view of Alfred J. Menezes, HANDBOOK OF APPLIED CRYPTOGRAPHY, Chapter 7, Block Ciphers (CRC Press LLC 1997) ("Menezes"). In this response, Applicant proposes to amend claims 42, 69, and 77. Support for these proposed amendments can be found in the originally-filed specification at, for example, p. 10, ll. 20-36 and Figs. 5-6. No new matter has been added. Accordingly, claims 42-82 are currently pending, of which claims 42, 69, and 77 are independent. Applicant respectfully traverses all pending rejections and requests reconsideration of the application, as amended.

Rejection Under 35 U.S.C. § 112, ¶ 1

Applicant traverses the rejection of claim 42-82 under 35 U.S.C. § 112, ¶ 1 for failing to comply with the written description requirement. The Final Office Action alleges that the recitation of "wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input" in independent claims 42 and 69 is not supported by the

¹ The Final Office Action contains a number of statements characterizing the Applicant's disclosure, including the claims, and the related art. Regardless of whether any such statement is specifically addressed herein, Applicant declines to automatically subscribe to any statement or characterization in the Final Office Action.

originally-filed specification. In addition, the Final Office Action alleges that the recitation of “by inputting said selected k bits into a transformation circuit without also inputting said first portion m of bits into said transformation circuit” in independent claim 77 is not supported by the originally-filed specification. See Final Office Action, pp. 2-4. Applicant respectfully disagrees with these assertions.

“To satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention.” M.P.E.P. § 2163(I) (8th ed., rev. 7, July 2008). Although “newly added claim limitations must be supported in the specification through express, implicit, or inherent disclosure,” “there is no *in haec verba* requirement” *Id.* In addition, the M.P.E.P. advises that “a lack of literal basis in the specification for a negative limitation may not be sufficient to establish a *prima facie* case for lack of descriptive support.” *Id.* at § 2173.05(i).

Applicant respectfully submits that the originally-filed specification expressly, implicitly, and/or inherently describes “without receiving said first portion of said input block of bits as an input,” as recited in independent claims 42 and 69 and “without also inputting said first portion m of bits into said transformation circuit,” as recited in independent claim 77. For example, at least page 6, line 29 to page 7, line 15, page 10, lines 20-33, Fig. 1, and Fig. 5 disclose exemplary embodiments in which bits input into a generic building block of a secret-key-controlled reversible logic circuit are divided into two groups of m control bits and n transformed bits. The m control bits are used to select k secret key bits out of $2^m k$ bits by a multiplexer and are also passed to the output of the building block intact. These portions of the specification further disclose that only

the remaining n bits and the k secret key bits are input into a transformation circuit, which outputs n transformed bits. Applicant submits that these disclosures of inputting only the n remaining bits and the k secret key bits into the transformation circuit would be understood by a person having ordinary in the art as describing “without receiving said first portion of said input block of bits as an input,” as recited in independent claims 42 and 69 and “without also inputting said first portion m of bits into said transformation circuit,” as recited in independent claim 77. Therefore, the originally-filed specification fully supports the above-referenced recitations in independent claims 42, 69, and 77. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the claim rejection under 35 U.S.C. § 112, first paragraph.

Rejections Under 35 U.S.C. § 103(a)

Applicant respectfully traverses the rejection of claims 42-82 under 35 U.S.C. § 103(a) as being unpatentable over Viktor in view of Matsui and further in view of Menezes. The Final Office Action has not properly resolved the *Graham* factual inquiries, the proper resolution of which is the requirement for establishing a framework for an objective obviousness analysis. See M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 U.S.P.Q. 459 (1966), as reiterated by the U.S. Supreme Court in *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 82 U.S.P.Q.2d 1385 (2007).

While Applicant proposes to amend independent claims 42, 69, and 77 to further demonstrate the differences between Menezes and the claims, Applicant maintains that the Final Office Action has not properly ascertained the differences between the claims and the references, at least because it has not interpreted the references and

considered both the claims and the prior art as a whole. See M.P.E.P. § 2141(II)(B).

Accordingly, the Final Office Action does not clearly articulate a reason why the claimed invention would have been obvious, which is “[t]he key to supporting any rejection under 35 U.S.C. 103.” M.P.E.P. § 2143.

Representative claim 42, as proposed to be amended, calls for a combination including, for example, “a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits . . . wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input and said output block of bits comprises the transformed bits followed by said first portion of said input block of bits.” Applicant respectfully submits that neither Viktor, Matsui, nor Menezes, either alone or in combination, teaches or suggests at least this element of Applicant’s amended independent claim 42.

The Final Office Action concedes that “Viktor fails to disclose ‘. . . a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits . . . wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input.’” Final Office Action, p. 5. Applicant submits that because Viktor does not teach or suggest this claim element, it also cannot teach or suggest “a transformation circuit . . . wherein . . . said output block of bits comprises the transformed bits followed by said first portion of said input block of bits” as recited by amended independent claim 42.

Moreover, Matsui does not cure Viktor's deficiencies. The Final Office Action relies on Matsui for its alleged teaching of a transformation circuit, but concedes that Matsui does not teach or suggest a transformation circuit "wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input." See Final Office Action, pp. 6-7. Applicant submits that because Matsui does not teach or suggest this claim element, it also cannot teach or suggest "a transformation circuit . . . wherein . . . said output block of bits comprises the transformed bits followed by said first portion of said input block of bits" as recited by amended independent claim 42. More specifically, because the alleged transformation circuit of Matsui does not "transform[] said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input," the output block of bits of its transformation circuit cannot constitute "the transformed bits followed by said first portion of said input block of bits" as recited by amended independent claim 42.

Finally, Menezes does not cure the above-referenced deficiencies of Viktor and Matsui. The Final Office Action relies on Menezes for its alleged disclosure of "a transformation circuit . . . wherein said transformation circuit transforms said remaining portion of said input blocks without receiving said first portion of said input block of bits as an input." More specifically, the Final Office Action appears to equate each round of the Feistel cipher of Menezes with the claimed "transformation circuit." See Final Office Action, p. 7 ("successive rounds of a Feistel cipher operate on alternating halves of the ciphertext, while other remains constant"). Even assuming this is correct, which Applicant does not concede, Menezes still does not teach or suggest "a transformation

circuit . . . wherein . . . said output block of bits comprises the transformed bits followed by said first portion of said input block of bits,” as required by amended claim 42.

Menezes generally discloses “[a]n *iterated block cipher* [,which] is a block cipher involving the sequential repetition of an internal function called a *round function*.”

Menezes, p. 251 (emphasis in original). Menezes further discloses a Feistel cipher as an example of an iterated block cipher. More specifically, Menezes discloses that

*A Feistel cipher is an iterated cipher mapping a 2l-bit plaintext (L_0, R_0) , for t-bit blocks L_0 and R_0 , to a ciphertext (L_r, R_r) , through an r-round process where $r \geq 1$. For $1 \leq i \leq r$, round i maps $(L_{i-1}, R_{i-1}) \rightarrow (L_i, R_i)$ as follows: $L_i = R_{i-1}$, $R_i = L_{i-1} [\text{XOR}] f(R_{i-1}, K_i)$, where each *subkey* K_i is derived from the cipher key K .*

Id. at p. 251 (emphasis in original).

Menezes fails to disclose or suggest “a transformation circuit . . . wherein . . . said output block of bits comprises the transformed bits followed by said first portion of said input block of bits,” as required by amended claim 42. Instead, Menezes discloses that the output of each round, which the Final Office Action appears to equate to the claimed transformation circuit, comprises a block of bits in which untransformed bits are followed by transformed bits. As noted above, Menezes discloses that each “round i maps $(L_{i-1}, R_{i-1}) \rightarrow (L_i, R_i)$ as follows: $L_i = R_{i-1}$, $R_i = L_{i-1} [\text{XOR}] f(R_{i-1}, K_i)$.” Menezes, p. 251. In other words, Menezes discloses that $(L_{i-1}, R_{i-1}) \rightarrow (L_i = R_{i-1}, R_i = L_{i-1} [\text{XOR}] f(R_{i-1}, K_i))$. So, for example, following this equation for $i=1$, as in the first round of the Feistel cipher, the input bits to the round correspond to (L_0, R_0) , and the output bits of the round correspond to $(R_0, L_0 [\text{XOR}] f(R_0, K_1))$. Thus, in Menezes the output block of bits of each round correspond to the untransformed input bits, R_0 , followed by the transformed bits, $L_0 [\text{XOR}] f(R_0, K_1)$. Accordingly, Menezes does not teach or suggest “a transformation

circuit . . . wherein . . . said output block of bits comprises the transformed bits followed by said first portion of said input block of bits," as required by amended claim 42.

As set forth above, Viktor, Matsui, and Menezes do not teach or suggest every feature of Applicant's amended independent claim 42. Consequently, the Final Office Action has not properly ascertained the differences between the references and the rejected claim. Accordingly, no reason has been clearly articulated as to why the claim would have been obvious to one of ordinary skill in the art. For at least this reason, claim 42 should be allowable.

Applicant's amended independent claims 69 and 77, although different in scope from amended independent claim 42, recite similar subject matter and are therefore allowable for at least the same reasons. Dependent claims 43-68, 70-76, and 78-82, each depend from one of independent claims 42, 69, and 77, and are therefore allowable for at least the same reasons. Applicant therefore respectfully requests that the rejection of claims 42-82 under 35 U.S.C. § 103(a) be withdrawn.

Conclusion

Applicant respectfully requests that this Amendment under 37 C.F.R. § 1.116 be entered by the Examiner, placing claims 42-82 in condition for allowance. Applicant submits that the proposed amendments of claims 42, 69, and 77 do not raise new issues or necessitate the undertaking of any additional search of the art by the Examiner, since all of the elements and their relationships claimed were either earlier claimed or inherent in the claims as examined. Therefore, this Amendment should allow for immediate action by the Examiner.

Furthermore, Applicant respectfully points out that the final action by the Examiner presented some new arguments as to the application of the art against Applicant's invention. It is respectfully submitted that the entering of the Amendment would allow the Applicant to reply to the final rejections and place the application in condition for allowance. Finally, Applicant submits that the entry of the amendment would place the application in better form for appeal, should the Examiner dispute the patentability of the pending claims.

In view of the foregoing remarks, Applicant submits that this claimed invention, as amended, is neither anticipated nor rendered obvious in view of the prior art references cited against this application. Applicant therefore requests the entry of this Amendment, the Examiner's reconsideration and reexamination of the application, and the timely allowance of the pending claims.

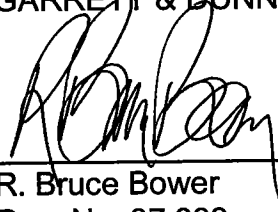
Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: August 26, 2009

By: _____


R. Bruce Bower
Reg. No. 37,099